AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Minnesota

GARY HALL, on behalf of himself and all others similarly situated

Plaintiff(s)

v.

CENTERSPACE, LP and CENTERSPACE INC.

Defendant(s)

Civil Action No. 22-cv-02028

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* CENTERSPACE INC.
c/o Corporation Service Company
2345 Rice Street, Suite 230
Roseville, MN 55113

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Raina C. Borrelli (raina@turkestrauss.com)
TURKE & STRAUSS LLP
613 Williamson St., Suite 201, Madison, Wisconsin 53703
Telephone: (608) 237-1775, Facsimile: (608) 509-4423

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 22-cv-02028

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Minnesota

GARY HALL, on behalf of himself and all others similarly situated

Plaintiff(s)

v.

CENTERSPACE, LP and CENTERSPACE INC.

Defendant(s)

Civil Action No. 22-cv-02028

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* CENTERSPACE, LP
c/o Corporation Service Company
2345 Rice Street, Suite 230
Roseville, MN 55113

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Raina C. Borrelli (raina@turkestrauss.com)
TURKE & STRAUSS LLP
613 Williamson St., Suite 201, Madison, Wisconsin 53703
Telephone: (608) 237-1775, Facsimile: (608) 509-4423

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 22-cv-02028

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

GARY HALL, on behalf of himself and all others similarly situated, Plaintiff, v. CENTERSPACE, LP and CENTERSPACE INC. Defendants.	Case No. 22-cv-02028 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Gary Hall ("Mr. Hall"), through his attorneys, brings this Class Action Complaint against the Defendants, Centerspace, LP and Centerspace, Inc. ("Centerspace" or "Defendants"), and their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, alleging as follows:

INTRODUCTION

1. Centerspace is a real estate company focused on the ownership, management, acquisition, and redevelopment of apartment communities across the Midwest but predominantly in Minneapolis, Minnesota.

2. Centerspace lost control over consumers' and employees' highly sensitive personal information when cybercriminals infiltrated Centerspace's unprotected or negligently-protected computer systems ("Data Breach")—and then waited eight months to tell them about it.

3. On November 11, 2021, Centerspace discovered that cybercriminals accessed and acquired files containing consumers' and employees' "personally identifiable information" ("PII"), including their names, Driver's License Numbers, and Social Security Numbers.

4. The Data Breach impacted 8,190 individuals, including current and former employees and current and former tenants and prospective tenants, and their PII.

5. Centerspace requires prospective tenants, tenants, prospective employees, and employees to disclose their PII to receive housing and employment. In so doing, Centerspace implicitly promises to safeguard their PII from hackers.

6. Under state and federal law, companies like Centerspace have duties to protect consumers' PII and to notify them about breaches "without unreasonable delay."

7. In fact, Minnesota requires that notice to individuals about a data breach "must be made in the most expedient time possible and without unreasonable delay." Minn. Stat. § 13.055, subd. 2(a); *see also* Minn. Stat. § 325E.61, subd. 1(a) (requiring the same notice "in the most expedient time possible and without unreasonable delay"); Minn. Stat. § 325E.61, subd. 1(b) ("Any person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data *immediately following discovery*, if the personal information was, *or is reasonably believed to have been, acquired by an unauthorized person*.") (emphasis added).

8. Centerspace recognizes these duties, informing its tenants and employees that "Centerspace takes the privacy and security of all information within its possession very seriously."[1]

9. It is unknown for how long the hackers had access to Centerspace's computer systems before the breach was discovered on November 11, 2021, meaning Centerspace had no effective means to prevent, detect, stop, or mitigate breaches of its systems, allowing cybercriminals unfettered access to consumer PII.

[1] A true and correct copy of the Breach Notice is attached hereto as **Exhibit A**.

10. On information and belief, cybercriminals were able to breach Centerspace's systems because it does not adequately train its employees on cybersecurity or maintain reasonable security safeguards or protocols to protect its tenants' and employees' PII, leaving it an unguarded target for theft and misuse.

11. After the Data Breach, Centerspace waited nearly eight months to notify consumers about it, leaving consumers in the dark and depriving them an opportunity to mitigate the Data Breach's effects on them.

12. It is unclear why Centerspace waited so long to notify its tenants and employees when it knew "[b]eginning on November 15, 2021, . . . that files potentially containing personal information may have been accessed or acquired by an unauthorized third-party in connection" with the Data Breach.[2]

13. And when Centerspace finally announced the Data Breach in July 2022, it deliberately downplayed how devastating it was, telling consumers "Centerspace is not aware of any misuse of your information as a result of this incident," even though cybercriminals misused it by accessing it without their permission.[3]

14. What's more, despite waiting eight months to disclose the Data Breach to unsuspecting employees and tenants, Centerspace was unable or unwilling to disclose exactly how the Data Breach happened, what information hackers stole from which consumers, who the hackers were, whether Centerspace knows if the PII was posted online for sale, and why it took Centerspace eight months to issue a bare-bones notice.

15. Centerspace's conduct violated Minnesota law and harms thousands of its own tenants and employees.

---

[2] *Id.*
[3] *Id.*

16. Centerspace knew or should have known that the Data Breach's victims deserved adequate and timely notice of the Data Breach and assistance in mitigating the effects of the Breach.

17. Plaintiff is a Data Breach victim, receiving a breach notice on July 18, 2022. Mr. Hall brings this Class Action on behalf of himself and all others harmed by Centerspace's misconduct.

18. Centerspace's misconduct has injured Mr. Hall and members of the proposed Class, including: (i) costs associated with the prevention, detection, and recovery from fraudulent charges, and other unauthorized use of their data; (ii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iii) emotional distress associated with the loss of control over their PII.

19. On information and belief, the employee and tenant information and PII compromised in the Data Breach is still stored in Centerspace's systems. Mr. Hall and members of the proposed Class have an interest in ensuring that their information is safe, entitling them to seek injunctive and other equitable relief, including independent oversight of Centerspace's security systems.

PARTIES

20. Plaintiff, Gary Hall, is a natural person and citizen of South Dakota, residing in Sioux Falls, South Dakota, where he intends to remain. Mr. Hall is a Data Breach victim, receiving Centerspace's Breach Notice in July 2022.

21. Defendant, Centerspace, is a North Dakota Limited Partnership, with its principal place of business at 3100 10th Street SW, Sharon Cargo, Minot, North Dakota 58701 and its

headquarters located at 800 LaSalle Plaza, Suite 1600, Minneapolis, Minnesota, 55402.[4]

22. Defendant Centerspace, Inc., is a North Dakota Corporation, with its principal place of business at 3100 10th Street SW, Minot, North Dakota 58701.

JURISDICTION & VENUE

23. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiff and Defendants are citizens of different states. There are more than 100 putative members of the Class.

24. This Court has jurisdiction over Defendants because they are headquartered in Minnesota, regularly conduct business in Minnesota, and have sufficient minimum contacts in Minnesota.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants' headquarters is in this District, Defendants maintain an office in this District and has a registered agent in this District, and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND FACTS

a. Centerspace

26. Centerspace is an owner and operator of apartment complexes. Founded in 1970, Centerspace owns 62 apartment complexes consisting of 11,579 apartments located in Colorado, Minnesota, Montana, Nebraska, North Dakota, and South Dakota.

[4] A true and correct copy of Centerspace's Notice of Data Security Incident to the Maine Office of the Attorney General is attached hereto as **Exhibit B**. *See also* 2021 Annual Report, https://s23.q4cdn.com/320605875/files/doc_financials/2021/ar/2021-Annual-Report.pdf (last accessed August 3, 2022) ("We conduct our corporate operations from offices in Minot, North Dakota and Minneapolis, Minnesota.").

27. On information and belief, Centerspace also employs property managers at each of its apartment complexes through its subsidiary, IRET. Plaintiff is a former employee of IRET Property Management.

28. Centerspace requires its residents and prospective residents to disclose their PII when collecting housing applications. Centerspace requires its current and former employees to disclose their PII when collecting job applications and onboarding information. Centerspace requires the disclosure of and collects this PII as a condition of providing housing and employment.

29. This PII includes their names, Social Security Numbers, driver's license numbers, and financial account numbers.

b. Centerspace Fails to Guard Consumer PII

30. In collecting and maintaining the PII, Centerspace agreed it would safeguard the data according to its internal policies and state and federal law.

31. Centerspace failed in that duty.

32. On November 11, 2021, Centerspace discovered that unauthorized third parties gained access to its computer systems. After hiring independent digital forensics and an incident response firm to determine what happened, it took four days, until November 15, 2021, for Centerspace to determine that files containing PII were accessed or acquired by the cybercriminals.

33. It is unknown for how long the hackers had access to the PII belonging to Centerspace's tenants and employees, both current, former, and prospective.

34. It took another seven-and-a-half months, until July 1, 2022, for Centerspace and its purported expert team of investigators, to determine whose PII was contained in the files

accessed or acquired by the cybercriminals.

35. On information and belief, Centerspace failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over consumer PII. Centerspace's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that Centerspace cannot, or will not, determine the full scope of the Data Breach, as it has been unable to determine exactly what information was stolen and when.

36. What's more, Centerspace was unable or unwilling to notify its employees and tenants about the Data Breach "without unreasonable delay" as required under Minnesota law, instead taking nearly eight months to notify victims.

37. After the Data Breach, "Centerspace implemented measures to enhance the security of its digital environment in an effort to minimize the likelihood of a similar event occurring in the future,"—measures that should have been in place *before* the Data Breach.

c. Plaintiff's Experience

38. Mr. Hall is a former employee of IRET Property Management, which is a subsidiary of Centerspace.[5]

39. As a condition of employment with Centerspace, Centerspace requires consumers to disclose their PII, including names, bank account information, and Social Security Number.

40. Mr. Hall provided his PII to Centerspace and trusted that the company would use

[5] *See* https://ir.centerspacehomes.com/corporate-overview/press-releases/news-details/2020/IRET-Announces-Minneapolis-Investment-Activity/default.aspx (last accessed August 3, 2022); see also 2021 Annual Report, https://s23.q4cdn.com/320605875/files/doc_financials/2021/ar/2021-Annual-Report.pdf (last accessed August 3, 2022) ("[Centerspace] conduct our daily business operations primarily through our operating partnership, Centerspace, LP, formerly known as IRET Properties (the "Operating Partnership"). The sole general partner of Centerspace, LP is Centerspace, Inc., formerly known as IRET, Inc., a North Dakota corporation and our wholly owned subsidiary.").

reasonable measures to protect it according to Centerspace's internal policies and state and federal law.

41. Mr. Hall has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Mr. Hall fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Mr. Hall has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

d. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

42. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendants.

43. As a result of Centerspace's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent

researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PII in their possession.

44. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

45. The value of Plaintiff and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

46. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

47. One such example of criminals using PII for profit is the development of "Fullz" packages.

48. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

49. The development of "Fullz" packages means that stolen PII from the Data Breach

can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

50. Defendants disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

51. Defendants' failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

e. Defendants failed to adhere to FTC guidelines.

52. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendants, should

employ to protect against the unlawful exposure of PII.

53. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

54. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

55. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

56. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. Defendants' failure to employ reasonable and appropriate measures to protect

against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

58. Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach disclosed by Centerspace in July 2022.

Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

59. Plaintiff reserves the right to amend the class definition.

60. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

a. **Numerosity**. The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class includes at least 8,190 members.

b. **Commonality and Predominance**. Plaintiff and the Class's claims raise predominantly common fact and legal questions, which predominate over any questions affecting individual Class members, that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff and the Class's PII;

ii. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendants were negligent in maintaining, protecting, and securing PII;

iv. Whether Defendants breached contract promises to safeguard Plaintiff and the Class's PII;

v. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendants' Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff and the Class injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

c. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class members' interests. They have also retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Superiority.** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial

detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendants. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

61. Plaintiff reallege all previous paragraphs as if fully set forth below.

62. Plaintiff and members of the Class entrusted their PII to Defendants. Defendants owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

63. Defendants owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff' and members of the

Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

64. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendants also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

65. Defendants owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendants actively sought and obtained Plaintiff' and members of the Class's personal information and PII.

66. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

67. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customers' and employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff and the members of the Class's

sensitive PII.

68. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

69. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendants hold vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the PII—whether by malware or otherwise.

70. PII is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class's and the importance of exercising reasonable care in handling it.

71. Defendants breached their duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff and members of the Class's injury. Defendants further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages,

increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

72. Defendants' breach of their common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Breach of an Implied Contract
(On Behalf of Plaintiff and the Class)

73. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

74. Defendants offered to employ Plaintiff and members of the Class in exchange for their PII. Defendants also offered to provide housing for members of the Class in exchange for their PII.

75. In turn, and through internal policies, Defendants agreed they would not disclose the PII it collects to unauthorized persons. Defendants also promised to safeguard PII.

76. Plaintiff and the members of the Class accepted Defendants' offers by disclosing their PII to Defendants in exchange for employment and housing with Defendants.

77. Implicit in the parties' agreement was that Defendants would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

78. Plaintiff and the members of the Class would not have entrusted their PII to

Defendants in the absence of such agreement with Defendants.

79. Defendants materially breached the contract(s) it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendants further breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendants created, received, maintained, and transmitted.

80. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendants' material breaches of their agreement(s).

81. Plaintiff and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendants.

82. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

83. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of

inaction, and fair dealing may require more than honesty.

84. Defendants failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

85. In these and other ways, Defendants violated its duty of good faith and fair dealing.

86. Plaintiff and members of the Class have sustained damages because of Defendants' breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

87. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

88. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

89. Plaintiff and members of the Class conferred a benefit upon Defendants by paying, in part, for Defendants to protect the PII they collected.

90. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and members of the Class. Defendants also benefited from the receipt of Plaintiff and members of the Class's PII, as this was used to provide its goods and services.

91. Under principals of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff and the proposed Class's services and their PII because Defendants failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII to Defendants had they known Defendants would not adequately

protect their PII.

92. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

COUNT IV
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

93. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

94. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

95. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendants' common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff alleges Defendants' actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

96. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII with which it is entrusted, and to notify impacted

individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendants breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' and employees' personal and financial information; and

c. Defendants' breach of its legal duty continues to cause harm to Plaintiff and the Class.

97. The Court should also issue corresponding injunctive relief requiring Defendants to employ adequate security protocols consistent with industry standards to protect its clients' (i.e. Plaintiff's and the Class's) data.

98. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendants' data systems. If another breach of Defendants' data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

99. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued.

100. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus

eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: August 17, 2022

Respectfully submitted,

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
Samuel J. Strauss
Brittany Resch
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com
brittanyr@turkestrauss.com